REMARKS

The Official Action dated March 31, 2003 has been received and carefully noted. The period for response having been extended from June 30, 2003 until July 31, 2003 by the attached Petition for Extension of Time, the above amendments and the following remarks are submitted as a full and complete response thereto.

Various of claims 1-56 and 111-125 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is added, and no new issues are raised which require further consideration and/or search. It is respectfully submitted that the above amendments, and the following remarks, are submitted to place this application in condition for allowance.

The response which was filed on March 4, 2003, was successful in overcoming all of the rejections noted in the previous Office Action, with the exception of a statutory subject matter rejection under 35 USC § 101. Claims 1-56 and 111-125 were rejected under 35 USC § 101, on the grounds that the claims, as submitted on March 4, 2003, were directed to non-statutory subject matter. Applicants respectfully traverse this rejection, and submit that the above amendments further clarify that the subject matter of the invention is in compliance with United States patent practice, in compliance with 35 USC § 101, and in compliance with the guidelines regarding computer-implemented inventions as set forth in MPEP § 2106.

I. CLAIMS ARE DIRECTED TO STATUTORY ARTICLE OF MANUFCTURE:

MPEP § 2106 clearly states that claims which are directed to an article of manufacture is in fact statutory subject matter. The article of manufacture of the present claims, which is a storage medium accessed by various computers or accessible by a computer, is recited as comprising various types of data thereupon. Although the claims as submitted on March 4, 2003, recited a specific interrelationship between the data and the computer, the presently pending claims have been amended to more particularly recite that the storage medium includes either a storage area containing encrypted electronic data, or encrypted electronic data which is to be <u>decrypted by a computer</u>. All of the claims recite interaction with either a first computer and a second computer, a vendor computer and a user computer, or other computers which interrelate with the storage medium in the particular manners recited in the claims.

The Office Action also took the position that "usefulness under the patent eligibility standard requires significant functionality to be present to satisfy the useful result aspect of the practical application requirement...Merely claiming non-functional descriptive material stored in a computer-readable medium does not make the invention eligible for patenting." The Office Action cites the 1992 CAFC case of *Arrhythmia Research Technology Inc. v. Corazonix Corp.*, 22 USPQ 2d 1033, 1036 (Fed. Cir. 1992) as providing authority for these statements. However, applicants respectfully submit that the *Arrhythmia* case does not support this holding. It should be noted that the *Arrhythmia*

case was decided on March 12, 1992, and the "useful, concrete, and tangible result" requirement for business method and software-type inventions was not developed until the _State Street Bank_ case was decided in 1998 (_State Street Bank v. Signature Financial Group, Inc._, 149 F.3d 1368, 47 USPQ 2d 1596, (Fed. Cir. 1998)). The _Arrhythmia_ case at the relied-upon page 1036, merely contains a discussion of older and significantly modified decisions regarding computer programs and patentability which are not applicable to the case at hand. In _Arrhythmia_, the court held United States Patent Number 4,422,459 to be <u>valid</u> since the claim recited a series of steps which processed signals. Though the facts of _Arrhythmia_ are not particularly applicable to the present case, _Arrhythmia_ does repeatedly say that the use of mathematical formulae or relationships to describe the structure or operation of an apparatus does not make it non-statutory. The present claims, being clearly directed to an article of manufacture, should be considered to be statutory subject matter.

II. <u>THE CLAIMS RECITE FUNCTIONAL RELATIONSHIPS BETWEEN THE DATA ON THE STORAGE MEDIUM AND THE COMPUTER, AND THE AREAS OF DATA ON THE STORAGE MEDIUM</u>:

Though the claims are directed to a storage medium, the Office Action takes the position that the claims did not recite a sufficient functional relationship between either the elements of the storage medium themselves, and/or the elements of the storage medium and the computer. However, applicants respectfully submit that under the current state of the law, the claims recite areas or data on a computer storage medium

which imparts specific functionality to the computer, and which provides a useful, concrete, and tangible result as required by United States patent law. Further amendments have been made to more clearly support this fact.

Using claim 1 as an example, the storage medium is recited as being accessed by a vendor computer and a user computer, and comprises encrypted electronic data which is to be decrypted by the user computer, and the storage medium also contains a medium personal number. The medium personal number is recited as having particular characteristics, and is used for generating a decryption key for decrypting the encrypted electronic data in the user computer. Permission information and the medium personal number enables the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data.

The Office Action took the position that the description in the claims of a relationship between storage areas of the storage medium is an "abstract idea," and not a functional one which effects the computer or causes the computer to perform a stated functionality on any other data at a different storage area. The Office Action further cites § II of MPEP § 2106, and states that the claims as presented on March 4, 2003, did not recite a useful, concrete, and tangible result. However, applicants respectfully submit that MPEP § 2106 § IV(B)(1)(a) explains that when a computer program and presumably a data structure is recited in conjunction with a physical structure (in this application, a

storage medium and/or the user computer, second computer, etc.), Patent Office personnel should treat the claims as a <u>product</u> claim. Additionally, applicants respectfully submit that the MPEP clearly explains that data structures which are <u>not</u> claimed as embodied in computer readable media are descriptive material per se due to the fact that the claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention. However this same section of the MPEP does clearly state:

> "In contrast, a claimed computer-readable medium encoded with a data structure <u>defines</u> structural and functional interrelationships between the data structure and the computer software on hardware components which permit the data structures functionality to be realized, <u>and is thus statutory</u>." (Emphasis added)

Therefore, applicants strongly but respectfully submit that the Office Action seems to be ignoring the fact that the claims are clearly directed to a storage medium, and are not directed to computer programs or computer listings per se. MPEP § 2106 § IV(B)(2)(a) states that "a claim limited to a machine or manufacture, which has a practical application in the technological arts, is <u>statutory</u>." All of presently pending claims 1-56 and 111-125 clearly recite a storage medium which is accessible by a vendor computer and a user computer, with the various areas of the storage medium or the various data on the storage medium clearly interrelating and effecting each other, and clearly interrelating with and operating in conjunction with elements of the computer.

All of the claims clearly indicate that the encrypted electronic data is to be decrypted by the user computer, and is in fact decrypted by the user computer (or the second computer, etc.), in conjunction with a medium personal number, permission information, or other information as recited in the claims. Claims 1-56 and 111-125, as submitted herein, all recite the useful, concrete and tangible result of enabling the user computer or the second computer to decrypt the encrypted electronic data and/or the decryption key in the user computer without using a specific apparatus number for a specific computer.
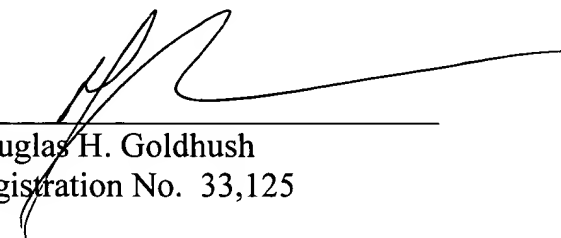
The useful, concrete and tangible result which is required by the *State Street Bank* Case (*State Street Bank v. Signature Financial Group, Inc.*, 149 F.3d 1368, 47 USPQ 2d 1596, (Fed. Cir. 1998), and *AT&T v. Excel Communications, Inc.*, 172 F.3d 1352, 50 USPQ 2d 1447 (Fed. Cir. 1999)), is clearly provided in the recited decryption of encrypted electronic data. The current state of the law regarding computer-implemented inventions is that as long as the inventions are new, useful, and non-obvious, and provide a useful, concrete, and tangible result, the invention should be found to be statutory subject matter, and should be found to be patentable. Additionally, in other CAFC cases in the last decade, the Court repeatedly held that a transformation of data within a computer system can constitute a practical application, and therefore should be found statutory subject matter under 35 USC§ 101 (see, for example, *In re Allapat* 33 F.3d 1526, 31 USPQ 2d 1545 (Fed. Cir. 1994), and *Arrythmia Research Technology, Inc. v. Corazonix Corp.*, 958 F.2d 1053, 22 USPQ 2d 1033 (Fed. Cir. 1992)).

Applicants appreciate the Examiner's consideration and courtesy to-date during the prosecution of this patent application. It is respectfully submitted that the above discussion regarding MPEP § 2106 and the supporting case law, and the above-noted clarifying amendments to the claims, make it clear that presently pending claims 1-56 and 111-125 are statutory subject matter under 35 USC § 101. It is therefore respectfully requested that the above amendments be entered, claims 1-56 and 111-125 be found allowable, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Douglas H. Goldhush
Registration No. 33,125

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DHG:scc

Enclosures: Marked-up Copy of Amended Claims
Petition for Extension of Time (1 month)

1. (Five Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer; and

permission information which includes the decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer, and generated based upon said medium personal number, said permission information and said medium personal number enabling the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data [enabling the user computer to decrypt said encrypted electronic data].

6. (Five Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating an encrypted permission information in said vendor computer; and

permission information encrypted in a manner that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number, wherein the permission information [enables the user computer to decrypt the encrypted electronic data] and said medium personal number enabling the user computer to decrypt the encrypted permission information and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted permission information and the encrypted electronic data.

11. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

encrypted permission information that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number;

wherein at least the medium personal number is written onto the storage medium in an unrewritable form which a user computer cannot rewrite, and wherein said encrypted permission information [enables the user computer to decrypt the encrypted electronic data] and said medium personal number enabling the user computer to decrypt the encrypted permission information and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted permission information and the encrypted electronic data.

17. (Five Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

encrypted electronic data to be decrypted by the user computer; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer and said medium personal number is used for generating a decryption key, said decryption key and said medium personal number enabling said user computer to decrypt said encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

18. (Five Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number is used for decrypting said encrypted electronic data; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer, said information [enabling said user computer to decrypt said electronic data] and said medium personal number enabling said user computer to decrypt the encrypted electronic

data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

19. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the second computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the

encrypted decryption key is generated independent from the specific apparatus number for the specific first computer,

wherein the encrypted decryption key in the third storage area <u>and said medium personal number</u> enables the second computer to decrypt the encrypted electronic data in the first storage area <u>in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data</u>.

23. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data based upon the decryption key and which stores the encrypted electronic data onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the encrypted decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the second computer, the encrypted electronic data includes electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the second computer to decrypt the encrypted electronic data in the first storage area in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

24. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

25. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data based upon the encrypted decryption key and which stores the encrypted electronic data onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

26. (Five Times Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon a medium personal number and independent from a specific apparatus number for a specific computer, and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

27. (Five Times Amended) A storage medium accessible from a vendor computer and a user computer at different times, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the user computer, the encrypted electronic data including electronic data encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly

personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer decrypts the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

28. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the user computer, the encrypted electronic data including electronic data encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted

decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area <u>and said medium personal number</u> enables the user computer to decrypt the encrypted electronic data in the first storage area <u>in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data</u>.

29. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second computer and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer, and wherein the encrypted decryption key and said medium personal number enables the second computer to decrypt the encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

33. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data to be decrypted by a specific second computer based upon the decryption key and which stores the encrypted electronic data onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for the specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific second computer, and wherein the encrypted decryption key <u>and said medium personal number</u> enables the second computer to decrypt the encrypted electronic data <u>in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data</u>.

34. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted

decryption key is generated independent from the specific apparatus number for the specific computer; and

a storage area for storing encrypted electronic data to be decrypted by a user computer which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

35. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data to be decrypted by a user computer based upon the decryption key and which stores the encrypted electronic data onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer, and wherein the encrypted decryption key and said medium personal number enables the user computer to decrypt the encrypted

electronic data <u>in a manner that the user computer does not use the specific apparatus</u> <u>number for the specific first computer in decrypting the encrypted electronic data</u>.

36. (Five Times Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which enables a user computer to decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer; and

a storage area for storing encrypted electronic data which is accessible after the decryption key has been decrypted, wherein said decryption key <u>and said medium</u> <u>personal number</u> enables the user computer to decrypt the encrypted electronic data <u>in a</u>

manner that the user computer does not use the specific apparatus number for the specific

first computer in decrypting the encrypted electronic data.

37. (Five Times Amended) A storage medium accessible from a vendor computer

and a user computer at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from

the computers, wherein the medium personal number is particularly personal for each

storage medium and is different from a medium personal number of another storage

medium;

a storage area for storing an encrypted decryption key, wherein the encrypted

decryption key is generated based upon the medium personal number and the encrypted

decryption key is generated independent from a specific apparatus number for a specific

computer; and

a storage area for storing encrypted electronic data to be decrypted by the user

computer which is accessible after the decryption key has been decrypted, wherein said

decryption key and said medium personal number enables the user computer to decrypt

the encrypted electronic data in a manner that the user computer does not use the specific

apparatus number for the specific first computer in decrypting the encrypted electronic

data.

38. (Five Times Amended) A storage medium accessed by a vendor computer

and a user computer, said storage medium, comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer; and

a storage area for storing encrypted electronic data to be decrypted by the user computer which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

39. (Five Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted

based on the medium personal number and independent from the specific apparatus

number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable

from at least the second computers, wherein the medium personal number is particularly

personal for each storage medium and is different from a medium personal number of

another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second

computer, which includes data encrypted based upon the medium personal number and

encrypted independent from the specific apparatus number for the specific first computer,

wherein the second computer decrypts encrypted electronic data in a manner that

the second computer does not use the specific apparatus number for the specific first

computer in decrypting the encrypted decryption key and the encrypted electronic data.

43. (Five Times Amended) A storage medium accessible from a first computer

which encrypts a decryption key based upon a medium personal number and independent

from a specific apparatus number for a specific first computer and which stores the

encrypted decryption key onto the storage medium and which encrypts electronic data

based upon the decryption key and which stores the encrypted electronic data onto the

storage medium, and accessible from a plurality of second computers which decrypt the

encrypted decryption key stored on the storage medium based upon the medium personal

number and independent from a specific apparatus number for a specific second

computer and which decrypt encrypted electronic data stored on the storage medium

based upon the decryption key that has been decrypted based on the medium personal

number and independent from the specific apparatus number for the specific second

computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable

from at least the second computers, wherein the medium personal number is particularly

personal for each storage medium and is different from a medium personal number of

another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second

computer, which includes information encrypted based upon the medium personal

number and encrypted independent from the specific apparatus number for the specific

second computer,

wherein the second computer decrypts encrypted electronic data in a manner that

the second computer does not use the specific apparatus number for the specific second

computer in decrypting the encrypted electronic data.

44. (Five Times Amended) A storage medium accessible from a vendor computer

and a user computer, where the vendor computer encrypts a decryption key based upon a

medium personal number and independent from a specific apparatus number for a

specific computer and which stores the encrypted decryption key onto the storage

medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable,

wherein the medium personal number is particularly personal for each storage medium

and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user

computer wherein the encrypted electronic data includes information encrypted based

upon the medium personal number and encrypted independent from the specific

apparatus number for the specific computer,

wherein said user computer decrypts the encrypted electronic data in a manner that

the second computer does not use the specific apparatus number for the specific second

computer in decrypting the encrypted electronic data.

45. (Five Times Amended) A storage medium accessible from a first computer

which encrypts a decryption key based upon a medium personal number and independent

from a specific apparatus number for a specific computer and which stores the encrypted

decryption key onto the storage medium and which encrypts electronic data to be

decrypted by a user computer based upon the decryption key and which stores the

encrypted electronic data onto the storage medium, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable,

wherein the medium personal number is particularly personal for each storage medium

and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data wherein the encrypted

electronic data includes information encrypted based upon the medium personal number

and encrypted independent from the specific apparatus number for the specific computer,

wherein the user computer decrypts the encrypted electronic data <u>in a manner that</u>

<u>the second computer does not use the specific apparatus number for the specific second</u>

<u>computer in decrypting the encrypted electronic data</u>.

46. (Five Times Amended) A storage medium accessible from a plurality of

computers which decrypt an encrypted decryption key stored on the storage medium, the

encrypted decryption key being based upon the medium personal number and

independent from a specific apparatus number for a specific computer and which decrypt

encrypted electronic data stored on the storage medium based upon the decryption key

that has been decrypted based on the medium personal number and independent from the

specific apparatus number for the specific computer in a particular computer, comprising:

a storage area for storing the medium personal number, which is un-rewritable

from the computers, wherein the medium personal number is particularly personal for

each storage medium and is different from a medium personal number of another storage

medium; and

a storage area for storing encrypted electronic data to be decrypted by a user

computer wherein the encrypted electronic data includes information encrypted based

upon the medium personal number and encrypted independent from the specific

apparatus number for the specific computer,

wherein the user computer decrypts encrypted electronic data <u>in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data</u>.

47. (Five Times Amended) A storage medium accessible from different computers at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing encrypted electronic data to be decrypted by a user computer, which includes information encrypted based upon the medium personal number and encrypted independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted electronic data has been decrypted,

wherein the medium personal number enables a user computer to decrypt the encrypted electronic data <u>in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data</u>.

48. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing encrypted electronic data to be decrypted by the user computer which includes information encrypted based upon the medium personal number and encrypted independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted electronic data has been decrypted,

wherein the medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

49. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that encrypted electronic data

stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

53. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic data is encrypted based upon the decryption key and the encrypted electronic data is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the

medium personal number and independent from the specific apparatus number for the specific computer and that the encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular second computer in different time, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

54. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a

specific computer and that the encrypted decryption key is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

55. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic data is encrypted based upon the decryption key and the encrypted electronic data is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

56. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that an encrypted decryption key stored on the storage medium is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and encrypted electronic data stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user

computer, wherein the encrypted electronic data includes information encrypted based

upon the medium personal number and encrypted independent from the specific

apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user

computer to decrypt the encrypted electronic data in a manner that the user computer

does not use the specific apparatus number for the specific computer in decrypting the

encrypted decryption key encrypted electronic data.

111. (Four Times Amended) A storage medium accessed by a vendor computer

and user computer, said storage medium for storing information readable by said user

computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each

storage medium and is different from a medium personal number of another storage

medium, wherein at least the medium personal number is written onto the storage

medium in an un-rewritable form which the user computer cannot change; and

an area storing permission information which includes a decryption key encrypted

in a manner that is independent from a specific apparatus number for a specific computer

and based upon said medium personal number, wherein said permission information

[enables the user computer to decrypt the encrypted electronic data] and said medium

personal number enabling the user computer to decrypt the encrypted decryption key and

to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data.

112. (Four Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot rewrite; and

wherein the user computer decrypts the encrypted electronic data using permission information which is encrypted in a manner that is independent from a specific apparatus number for a specific computer and based upon said medium personal number.

113. (Five Times Amended) A storage medium accessed by a vendor computer and a user computer said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

wherein the user computer decrypts the encrypted electronic data using permission information that is encrypted independent from a specific apparatus number for a specific computer;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which a user computer cannot rewrite.

119. (Five Times Amended) A storage medium readable by a vendor computer and a user computer, said storage medium comprising:

data representing a medium personal number;

encrypted electronic data to be decrypted by the user computer; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the user computer decrypts the encrypted electronic data using the first data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

123. (Five Times Amended) A storage medium readable by a vendor computer and a user computer at different times, the storage medium comprising:

data representing a medium personal number;

encrypted electronic data to be decrypted by the user computer; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the user computer decrypts the encrypted electronic data using the first data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

124. (Four Times Amended) A storage medium for storing data for access and processing by a vendor computer and a user computer, said storage medium comprising:

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

an electronic information storage area including encrypted electronic data to be decrypted by the user computer; and

the user computer decrypts the encrypted electronic data based upon an encrypted decryption key which has been encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer .

125. (Four Times Amended) A storage medium for storing data for access and processing by a vendor computer and a user computer, said storage medium comprising:

an encrypted electronic data storage area including encrypted electronic data to be decrypted by the user computer;

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number enables decrypting of said encrypted electronic data from the user computer; and

wherein the user computer decrypts the encrypted electronic data based upon information which is encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.